Social Media Policy Study from Government Technology

In a study of 26 publicly available government social media documents, along with results from interviews with 32 government professionals already using or considering using social media tools, the CTG winnowed its findings down to eight essential elements to address for the use of social media. Those eight elements include employee access, account management, acceptable use, employee conduct, content, security, legal issues and citizen conduct. While these elements don't cover every possible issue (the guide is part of a larger project under way that focuses on government use of social media tools), it's a jump-off point:

1. Employee Access -- Not long ago, social media sites fell under the "non-work-related" umbrella, and thus governments tended to restrict access to these areas of the Internet. But those lines have blurred lately as personal, professional and official agency use of social media tools has become common, raising questions about whether employees should have access to social media sites and the proper means for gaining access.

Agencies are managing access in two ways: controlling the number and type of employees allowed access to social media sites or limiting the types of sites that are approved for employee access. Most agencies interviewed by the CTG restricted access to such sites, instead allowing access for only a handful of designated individuals or functions (such as leadership or public information officers).

But formal policies that specifically address access appear lacking: Of the 26 policies and guidelines CTG reviewed, only five specify access procedures. "Of those five, most required employees or departments to submit an official business case justification in order to access and use social media sites," the study said.

Based on its interviews, balancing unrestricted and controlled access is a dilemma for many agencies. "While some agencies may value the potential opportunities for professional development when employees are engaged in educational, collaborative or knowledge sharing activities fostered by open access to social media sites, many are still fearful of the perceived legal and security risks," the study said.

2. Account Management -- This entails the creation, maintenance and potential destruction of social media accounts. Lacking a policy for this could result in a situation where an agency's leadership is in the dark about what types of accounts are being established, maintained or closed by their employees for professional or official agency use, according to the study. In policies reviewed by the CTG, such strategies varied. One strategy required approval by only one designated party (most often the public information officer), while other agencies require approval by more than one party.

"While our sample of government policies is too small to draw any definite conclusions, local government policies tend to be more explicit on account management as compared to state or federal agencies," the study said.

3. Acceptable Use -- Such policies usually outline an organization's position on how employees are expected to use agency resources, restrictions on personal use and consequences of violating the policy. Twelve of the policies and guidelines reviewed by the CTG dealt with this specific issue, and the majority of them used existing policies that already dictated acceptable use of common electronic and information resources such as telephone, computer or Internet access.

This is perhaps one of the more disquieting, gray areas of social media policy, Hrdinová said, as it's difficult to make clear-cut distinctions between professional and personal use. For example, an employee may be Facebook friends with a CIO from another agency and chat in person and online about common interests, which may ebb and flow without much distinction from personal to professional. "But at the same time, are they strengthening the professional relationship?" she asks.

To illustrate the lack of policies surrounding acceptable personal use during designated times or nonwork hours, the CTG found that only three of the 26 policies have started addressing the issue.
For some agencies, the line isn't so blurry: Arvada, Colo., has a social media policy that clearly states, "Social media use is for corporate goals and objectives, not for personal use."
Others, like the U.S. Air Force, have more lenient policies and encourage their members to think of themselves as on duty 24/7 when it comes to social media use. Others suggested "acceptable employee use for professional interest is better monitored and managed by supervisors, rather than a one-size-fits-all policy.

4. Employee Conduct -- Most agencies reference existing policies by either using direct quotes or providing links or reference numbers on specific policies that address what is "right" and "wrong" as far as employees' behavior, and sets out consequences should a violation occur. However, none of the reviewed policies directly address the consequences of inappropriate conduct on personal social media sites, the CTG said.
In addition to standard conduct codes that address issues like racially offensive language, some policies address issues more specific to social media, including respecting the rules of the venue, striving for transparency and openness in interactions, and being respectful in all online interactions. "Other policies expressed an expectation of ‘trust' that employees will provide professional-level comments or content whether in their professional or personal lives," the study said.
While creating policies to address consequences of inappropriate use of social media tools is largely untouched territory, outlining which aspects are just recommendations for personal behavior and which are potential grounds for dismissal "might be useful for employees and their managers trying to navigate and define the parameters of the personal/professional divide," the study said.

5. Content -- Issues of who is allowed to post content on official agency social media sites and who is responsible for its accuracy came up frequently in the CTG's interviews. Fourteen of the reviewed documents address content management in some form. In many cases, such as Fairfax County, Va., content creation is given to the department or person who created the account, with the agency's public information officer being responsible for ensuring the accuracy of posted information and adherence to existing social media guidelines. But "the question of content management with respect to an employees' professional and personal use is left largely unexplored in policy and guideline documents," the study said.
More and more, professionals are engaging in work-related group discussions on sites like GovLoop and LinkedIn, and leaving online comments in response to work-related topics on external blogs, another concern for agencies. Ten of the 26 policies simply instruct their employees to always use a standard disclaimer that distances the employee's opinions and content from the official agency position. For example, the Air Force's social media policy and guidelines instruct employees to specify, through a disclaimer, that any comments provided by an employee on external social media sites are personal in nature and do not represent the views of the Air Force.

6. Security -- Agencies are trying to develop best practices to ensure security of their data and technical infrastructure in light of new uses, users and technologies related to social media. Some of the 26 policies deal explicitly with social media security concerns, while others are more general. For example, the Hampton, Va., policy points to existing IT security policies by stating, "Where appropriate, city IT security policies shall apply to all social networking sites and articles." Others target specific concerns: Two types generally found in the policies analyzed and discussed in interviews were technical and behavioral concerns. Technology concerns addressed in the policies focused on password security, functionality, authentication of identity using public key infrastructures and virus scans. Fifteen of the policies included specific requirements such as requiring users to maintain complex passwords, and a few policies required a designated official to hold all usernames and passwords for social media accounts. As

well, two policies detail how attachments should be scanned using anti-virus tools before being posted on behalf of the government.
Public-sector employees also may inadvertently post information about themselves or the agency on social media sites, which attackers then use to manipulate users. A related concern is the inadvertent posting of citizens' personal and protected information by agency employees. "While these concerns are not new, many of the reviewed policies mentioned the need to protect confidential information that is personally identifiable or could endanger the agency mission," the study said.

7. Legal Issues -- While some agencies' policies take a general approach to legal issues -- using generic text that requires all employees to adhere to applicable laws and regulations without specifying which are applicable -- others point to specific areas of law like privacy, freedom of speech, freedom of information, public records management, public disclosure and accessibility. Many agencies address the issue of records management and retention, but few include language related to the removal of records. Massachusetts, however, highlights the transitory nature of records in its guidelines on Twitter and gives instructions on how to download tweets from Twitter to prevent content loss.
Some agencies' policies proactively address potential legal issues by requiring using various disclaimers on social media sites like Hampton which directs its employees who engage on behalf of the city to "make clear that you are speaking on behalf of Hampton. If you publish content on any website outside of the city of Hampton and it has something to do with the work you do or subjects associated with the city, use a disclaimer such as this: 'The postings on this site are my own and don't necessarily represent the city's positions or opinions.'"

8. Citizen Conduct -- Grappling with instant two-way public communication between government and citizens is relatively new, and agencies must decide whether to allow such communication like comment boxes and how to handle that engagement. "For agencies that decide to elicit citizen feedback via their official agency social media sites, rules for acceptable conduct of citizens are often developed," the study said.
Eleven of the 26 policies and guidelines addressed this issue. Documents vary on how to deal with the content of such comments. "Some issue rules of conduct that are posted on the agency's site," the study said. "These rules generally refer to limitation on offensive language, inciting violence or promoting illegal activity. Similar rules are often already on agencies' websites and can be reused for social media purposes." But some policies, like Arvada's, simply detail who will have the responsibility of approving public comments without going into detail as to what makes a comment acceptable.
On top of the eight elements to effectively design a government social media policy, the CTG offers further guidance for those governments that are just getting started, including determining goals and objectives, forming a team, identifying existing policies that apply to using social media tools and discussing conflicts or inconsistencies between proposed, and existing policies and procedures.